



DIGITCOM SERVICES INC.  
5280 E. Beverly Blvd.  
Suite C, PMB 274  
Los Angeles, CA 90022  
310-861-6100

**Annual 64.2009(e) CPNI Certification for 2009 covering the prior Calendar year 2008**

Date filed: april 15<sup>th</sup>, 2010  
Name of Company: Digitcom Services Inc.  
Form 499a filer ID: 817130  
Name of Signatory: Luis Martinez  
Title of Signatory: CFO

I, Luis Martinez, certify that I am an officer of the company named above, and acting as agent of the company, that I have personal knowledge that the company has established operation procedures are adequate to ensure compliance with the Commission's CPNI rules.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping and supervisory review) set forth in section 64.2001 et seq of the Commission's rules.

The company has not taken action against data brokers in the year in question.

The company has not received customers complaints in the year in question concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47.C.F.R. & 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed

A handwritten signature in black ink, appearing to be "Luis Martinez", written over a horizontal line.

Attachments: Accompanying Statement explaining CPNU procedures.

**CPNI Procedures:**

- 1) Real time data protection:
  - a) Hourly monitoring of number of accounts a customer representative looks up
  - b) Credit card information hidden from all customer representatives
  - c) All data held in firewall protected servers
  - d) Automated alert systems that monitor access to customer accounts for unusual activity
  - e) DMZ data protection
  - f) Encrypted API protocol when connecting to Credit Card authenticator
  - g) Web page data is entered in 128/256 encrypted environment
  - h) Automated alert system to unauthorized intrusions or attempted intrusions into databases.
- 2) Fraud Investigation
  - a) Customer Service procedures to respond to customer concerns regarding their information
  - b) Full log in documentation of anyone accessing customer information